랜덤 부분 ID를 이용한 저비용 RFID 상호인증 프로토콜

준회원 이 영 진*, 정회원 문 형 진*, 정 윤 수*, 이 상 호**

Mutual Authentication Protocol Of The Low-cost RFID Using Random Partial ID

Yong-zhen Li* ***Associate Member***,
Hyung-Jin Mun*, Yoon-su Jeong*, Sang-ho Lee** ***Regular Members***

요 약

기존 RFID 기술은 리더와 태그사이에 물리적인 접촉 없이 인식 가능하고 태그의 정보가 전송과정에 무선특성에 따른 과도한 정보 노출과 사용자의 위치정보 추적과 같은 심각한 프라이버시 침해를 유발시킨다. 특히 읽기전용 태그에서의 보안문제는 단지 물리적 방법으로만 해결하고 있다. 이 논문에서는 간단한 XOR연산과 부분 ID를 이용하여 다양한 공격에 안전하며 읽기전용 태그에 적합한 저비용 인증 프로토콜을 제안한다. 제안 프로토콜은 재전송, 도청, 위장 및 위치 추적 등 공격에 안전하다.

Key Words : Partial ID, Low-cost RFID, Location Privacy, Authentication

ABSTRACT

Previous RFID technique, it is recognizable without the physical contact between the reader and the tag, causes the serious privacy infringement such as excessive information exposure and user's location information tracking due to the wireless characteristics. Especially the information security problem of read only tag is solved by physical method. In this paper, we propose a low-cost mutual authentication protocol which is adopted to read-only tag and secure to several attacks using XOR and Partial ID. The proposed protocol is secure against reply attacking, eavesdropping, spoofing attacking and location tracking.

Ⅰ. 서 론

RFID란 무선인식 기술 즉 Micro-chip을 내장한 태그(Tag), 레이블(Label), 카드(Card) 등에 저장된 데이터를 무선 주파수를 이용하여 리더(Reader)에서 자동으로 인식하게 하는 기술을 말한다. 또한 칩의 저장능력과 인식능력이 향상되면서 이 무선인식 기술은 유비쿼터스 환경에서 필수적인 기술로 각광을 받고 있다. RFID 기술은 단순한 바코드의 대체 수준을 넘어서 통신, 물류, 국방, 소방, 금융, 의료, 환경, 교육, 정보가전, 도로, 건설 등 다양한 인간의 생활 전반에 활용되어 무한한 부가가치를 창출 가능하여, 향후 전 세계적인 산업구조, 시장구조의 변화뿐만 아니라 인간의 삶의 형태까지 변화시키게 될 유비쿼터스 컴퓨팅의 기반 기술로서 인식되고 있다[1, 2].

그러나 RFID 기술은 리더와 태그사이에 물리적인 접촉 없이 인식 가능하고 태그의 정보가 전송과정에 무선특성에 따른 과도한 정보 노출과 사용자의 위치정보 추적과 같은 심각한 프라이버시 침해

* 충북대학교 전자계산학과 네트워크보안 연구실 (lyz2003@chungbuk.ac.kr)
** 충북대학교 전기전자컴퓨터공학부 및 컴퓨터정보통신연구소 (shlee@chungbuk.ac.kr)
논문번호 : KICS2006-03-106, 접수일자 : 2006년 3월 3일, 최종논문접수일자 : 2006년 6월 26일

를 유발시킨다. 이러한 우려들이 RFID의 상용화에 걸림돌이 되며, 성공적인 산업화를 위해서는 제반 프라이버시 문제를 해결해야 하는 것이 선결 과제로 되고 있다. 따라서 현재 태그에 저장된 정보를 보호하고 태그에 대한 위치추적 등과 같은 보안 문제를 해결을 위한 인증 프로토콜에 대한 연구가 활발히 진행되고 있다[3-5]. 그러나 지금까지 제안된 대부분의 인증 프로토콜은 읽기/쓰기가 가능한 태그들에만 적용 가능한 기법들이며 읽기 전용인 태그들에 대한 보안 기법은 거의 전무한 상태이다. 이는 읽기전용 태그를 비롯한 저가형 태그의 활용의 걸림돌로 되고 있다.

이 논문에서는 랜덤한 두개 부분 ID(PID: Partial ID)와 간단한 XOR연산을 이용하여 읽기전용 태그들로 구성된 RFID시스템에서도 적용 가능한 저비용 인증 프로토콜을 제안한다. 이 프로토콜은 기존 프로토콜에 비하여 자원소비를 최적화 하였고 또한 도청, 위장 및 프라이버시 침해와 같은 보안문제점을 해결하고자 한다.

논문의 구성은 다음과 같다. 2장에서는 기존 인증프로토콜에 대하여 분석하였고 3장에서는 제안프로토콜에 기술하며 4장에서는 제안프로토콜의 안전성과 효율성에 대하여 비교평가 하였으며 마지막 5장에서 결론을 맺도록 한다.

Ⅱ. 관련 연구

2.1 기존 RFID 인증 프로토콜

현재까지 RFID시스템에서 사용자의 프라이버시를 보호하기 위하여 여러 가지 기법들이 제안 되었다. 이런 기법들은 크게 태그 무효화(kill), Faraday Cage, Active Jamming 등 물리적 접근기법[7,8]과 비트연산(XOR) 기반, 해쉬함수 기반, 재 암호화 등 암호학적 접근기법으로 분류된다[1-6,10.11]. 지금 홈 네트워크나 유비쿼터스 환경에서는 주로 암호학적 접근기법을 사용하고 있다.

2.1.1 해쉬 기반 접근

(1) 해쉬 락 프로토콜 : 이 프로토콜에서는 그림 1에서와 같이 우선 태그에서 랜덤하게 선택된 Key의 해쉬 값인 metaID=h(key)를 이용하여 인증하는 방법이다. 이 기법은 고정된 metaID의 이용으로 태그의 추적이 가능하며 재전송 공격에 취약하다[1].

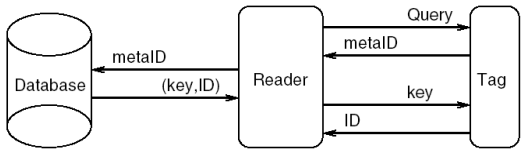

그림 1. 해쉬 락

(2) 랜덤 해쉬 락 프로토콜 : 이 프로토콜은 그림 2에서와 같이 해쉬 락 프로토콜의 확장기법으로 해쉬 함수와 의사난수 생성기를 갖는 태그는 h(ID‖R)과 랜덤값 R을 리더를 통하여 DB에 전달하여 DB에서 저장된 모든 ID와 R로부터 h(ID‖R)에 대응하는 식별 정보를 찾아낸 후 ID를 태그에게 전달하게 된다. 이 기법은 마지막 단계에서의 태그의 ID 노출되 가능성이 있고 또한 공격자가 R, H(ID,‖R)을 획득하여 재전송할 공격을 할 수 있다[2].

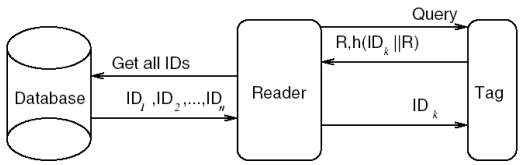

그림 2. 랜덤 해쉬 락

(3) 해쉬 체인 기법 : 이 기법은 그림 3에서와 같이 서로 다른 두개의 해쉬 함수를 이용하여 리더의 질의에 응답하여 At, I, G(Si) 정보를 전달하고 DB에서 G(Si)에 대한 i번의 인증연산을 거친 후 ID를 전달하게 된다. 그러나 해쉬 체인은 리더이 질의에 대해 항상 다른 응답을 하므로 공격자가 태그의 응답 αt,i를 알고 있으며 αt,i를 재전송 하는 경우 정당한 태그로 가장할 수 있으므로 재전송과 스푸핑 공격에 취약하다[6].

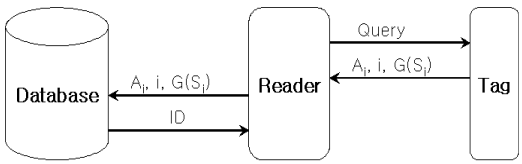

그림 3. 해쉬 체인 프로토콜

2.1.2 재 암호화 기법

재 암호화 기법은 최초로 Juels과 Pappu가 지폐의 시리얼 넘버를 공개키로 암호화하는 스킴을 제

안하였다. 공개키에 의해 암호화된 암호문은 주어진 태그의 연결성(linkability)을 감소시키기 위해 주기적으로 재암호화(re-encryption) 된다[8]. RFID 태그는 제한된 컴퓨팅 리소스를 가지기 때문에, 재 암호화는 외부의 계산 기관(computing agent)에서 수행한다. Golle et al.[9]은 소비자의 상품에 삽입된 RFID 태그의 프라이버시 보호에 보다 적합한 universal re-encryption 스킴을 제안하였다. 이 스킴은 여러 개의 공개키를 사용하며, 연관된 공개키의 정보 없이 암호문을 재 암호화하는 것이 가능한 ElGamal 암호의 확장이다. 그러나, 이 기법도 Juels과 Pappu의 기법과 마찬가지로 재암호화 디바이스에 대한 별도의 인프라가 필요하다는 단점이 있다.

2.1.3 XOR 기반 기법

(1) Juels 기법[10]

이 기법에서는 단지 XOR 연산을 사용하여 저가의 RFID 시스템에서 적용에 적합하다. 이 기법에서 태그는 리더로부터 이전 세션에서 받은 랜덤 값들과 현재 받은 랜덤 값들에 동일한 값을 가지고 있는지를 확인하여 상호인증을 한다. 구체적으로 보면 태그에는 $(\alpha_i, \beta_i, \gamma_i), 1 \leq i \leq k$로 구성된 비밀 값 k를 저장한다. 데이터베이스에는 전체 태그들에 관하 m개의 랜덤 값 $\Delta_i = \{\delta^{(1)}(=(\Delta\alpha_i^{(1)}, \Delta\beta_i^{(1)}, \Delta\gamma_i^{(1)})), \cdots, \delta^{(m)}\}, 1 \leq i \leq k$로 테이블을 구성하여 저장한다. 인증과정은 우선 리더가 태그에 질의하면 태그는 $\alpha_d, d \equiv (c \bmod k) + 1$(c는 초기값을 0인 카운터 수)를 리더에 전송한다. 리더는 α_d를 데이터베이스에 전송하여 와 α_d대응되는 β_d를 데이터베이스에서 받아 태그에 전송한다. 태그는 리더에서 받은 β_d와 자신이 저장하고 있던 β_d를 비교하여 리더를 인증하고 인가되면 태그는 다시 관련 γ_d를 리더를 통하여 데이터베이스에 전송하여 태그를 인증한다.

(2) Eunyoung기법

최은영 기법[11]은 Juels 기법을 기반으로 제안하였으며 특징은 태그와 데이터베이스에서 전송하는 값들과 비밀값들을 분리하여 처리하였다. 따라서 기존 Juels 기법보다 태그와 데이터베이스에서 적은 저장공간과 적은 계산량을 보여 효율적이다.

위의 XOR 기반 두 기법은 읽기/쓰기가 가능한 저가형 RFID태그에 적합하지만 추가되는 저장공간의 필요로 읽기전용 RFID태그에는 적용할 수 없다.

Ⅲ. 부분ID 기반 인증프로토콜

이 장에서는 부분ID를 사용하여 최저가의 태크에 적합한 안전한 인증프로토콜을 제안한다. 랜덤하게 선택된 부분ID 사용하여 태그의 위치노출을 막고 공격자의 무차별한 도청에 따른 데이터분석 및 위장공격에도 안전하다. 이 논문에서는 RFID 시스템을 간단하게 태그, 리더 및 백-엔드 데이터베이스로 구성한다고 가정한다.

3.1 RFID 시스템에서의 보안 요구사항

1) 도청공격에 안전해야 한다. 공격자가 리더와 태그간의 통신을 도청 가능하더라도 태그에 저장된 비밀정보를 알아내는 것이 불가능해야 한다.
2) 재전송 공격에 안전해야 한다. 공격자가 이전 세션의 모든 통신내용을 도청을 통하여 알고 있다고 하더라도 현재 세션에 통신될 정보를 생성하는 것이 불가능해야 한다.
3) 위장공격에 안전해야 한다. 공격자가 태그나 리더로 위장하여 태그 혹은 리더의 비밀정보를 알아내는 것이다. 즉 리더로 위장 시 태그의 비밀정보를 알아내기 위한 공격을 할 수 있으며 태그로 위장하여 재전송 공격 등이 가능하다.
4) 위치트래킹공격에 안전해야 한다. 공격자가 태그와 리더사이에 주고받는 정보를 분석하여 동일한 태그에서 전송되는 정보의 패턴을 알아내어 태그의 위치정보 나아가서 태그소유자의 위치정보를 알아내는 공격을 말한다. 읽기전용인 태그에서 이 공격을 막을 방법은 아직까지는 물리적이 방법을 취하고 있다.

3.2 PID를 이용한 RFID 인증프로토콜

3.2.1 초기화 단계

초기화 단계에서는 제안 프로토콜의 실행을 위한 준비단계로서 EPC 표준을 기반으로 태그, 리더 및 데이터베이스에서의 연산과 초기화 값들을 설정한다.

(1) 모든 태그에는 각각 자신의 비밀정보 SID(secure ID)를 저장한다.
(2) 리더에는 이사난수를 생성할 수 있는 난수 생성기를 설치한다.
(3) 그리고 데이터베이스에는 모든 태그의 비밀정보를 저장한다.

3.2.2 제안프로토콜의 실행과정

제안프로토콜은 그림 4에서 보는 바와 같이 11개 절차로 이루어진다.

① 리더가 랜덤 난수를 생성하여 질의정보와 함께 태그에 전송한다.

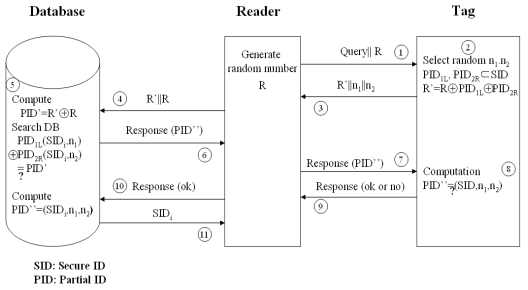

그림 4. 제안 프로토콜

② 태그는 랜덤 선택된 두수 n_1, n_2($L/2<n_1,n_2<L$)를 길이로 자신의 SID에서 왼쪽과 오른쪽으로부터 각각 지정길이의 PID_{1L}과 PID_{2R} 두개의 부분ID를 선정하고 선정된 PID_{1L}과 PID_{2R} 그리고 리더에서 받은 난수 R과 XOR하여 R'를 계산한다.

③ 태그는 계산한 R'과 랜덤 선택된 두수 n1, n2를 리더한테 전송한다.

④ 리더는 위에서 생성했던 난수 R과 태그에서 받은 전체 정보를 추가하여 데이터베이스에 전송한다.

⑤ 데이터베이스가 리더에게서 받은 R과 R'를 XOR하여 태그의 PID''=R⊕R'를 계산한다. 그리고 데이터베이스에서 PID'=Left(SID_i, n_1)⊕Right(SID_i, n_2)인 SID_i를 찾는다.

- 만일 검색한 결과 대응되는 SID_i가 없으면 태그를 위장된 태그로 인정한다. 만일 검색한 결과 대응되는 SID_i가 있다면 데이터베이스에서는 PID''=(SID_i, n_1, n_2)를 계산한다.

⑥ 데이터베이스는 계산한 PID''를 리더에게 전송한다.

⑦ 리더는 데이터베이스에서 받은 PID''를 태그에 전송한다.

⑧ 태그는 자신의 정보를 이용하여 Sub(SID_i, n_1, n_2)값을 계산하고 데이터베이스에서 받은 PID''와 동일 여부를 확인한다.

⑨ 만일 Sub(SID_i, n_1, n_2)값과 PID''값이 동일하면 리더에 "Ok" 응답을 보내고 그렇지 않으면 우리는 리더가 위장된 것으로 인정하고 리더에 "No" 응답을 보낸다.

⑩ 리더는 태그에서 "Ok"메시지를 받으면 그 정보를 데이터베시에 전송하고 "No"메시지를 받으면 프로토콜을 종료한다.

⑪ 데이터베이스는 "Ok"메시지를 확인하고 태그의 SID를 리더에게 제공한다.

3.2.3 태그와 리더의 상호인증

태그와 리더간의 상호인증은 그림 4에서의 제안 프로토콜 동작과정에서 자동으로 이루어진다.

리더가 태그에 대한 인증: 위의 프로토콜 동작과정 ⑤단계에서 PID'=Left(SID_i, n_1)⊕Right(SID_i, n_2)인 SID_i를 찾는다. 만일 검색한 결과 대응되는 SID_i가 없으면 태그를 위장된 태그로 인정하여 프로토콜을 중단하고 대응되는 SID_i가 있다면 정당한 태그로 인정한다.

태그가 리더에 대한 인증: 위의 프로토콜 동작과정 ⑧단계에서 태그는 자신의 정보를 이용하여 Sub(SID_i, n_1, n_2)값을 계산하고 데이터베이스에서 받은 PID''와 동일하면 정당한 리더로, 아니면 위장된 리더로 인정한다.

Ⅳ. 안전성 및 성능분석

4.1 안전성 분석

1) 재전송 공격에 대한 안전성 : 공격자는 리더로 위장한 재전송 공격과 태그로 위장한 재전송 공격 두 가지 경우가 있다. 리더로 위장한 경우 공격자는 리더에서 태그로 전송되는 메시지를 도청하여 재전송하는 경우인데 제안 프로토콜에서는 매번 태그에서 변화되는 정보PID_{1L}⊕PID_{2R} 와 리더에서 받은 랜덤 난수 R를 XOR하여 재전송 공격을 막는다.

2) 전송메시지의 기밀성 보장 : 기밀성 보장을 위하여 대부분 경우에 대칭키 암호기법을 이용한다. 하지만 RFID 태그는 저장공간과 연산능력의 제약으로 이런 암호화 기법을 사용하기에는 너무 많은 비용이 든다. 제안프로토콜에서는 난수와의 비트연산을 통하여 R⊕ PID_{1L}(=Left(SID, n_1))⊕PID_{2R}(=Right(SID, n_2))를 생성하여 전송메시지에 포함된 SID정보 관련 부분ID를 은닉시켜 전송하여 인증과정에 주고받는 메시지들의 기밀성을 보장한다. 난수와 자신의 SID 정보를 알고 있어야만 전송되는 태그의 부분 ID(PID_{1L}과 PID_{2R})를 계산해낼 수 있고 PID_{1L}(=Left(SID, n_1))⊕PID_{2R}(=Right(SID, n_2)), n1, n2가 노출된다 해도 태그의 전반 SID를 계산하는 것이 불가능하므로 메시지 도청공격에도 안전하다.

3) 위치 추적에 대한 안전성 : 태그와 리더사이에 주고받는 메시지가 모든 인증 단계에서 매번

표 1. 기존 인증프로토콜과의 안전성 기능비교

기법	위치추적	도청	재전송	계산량
해쉬락[1]	가능	×	×	해쉬 1회
랜덤해쉬락[2]	불가능	×	×	해쉬 1회
해쉬체인[6]	불가능	×	○	해쉬 2회
재암호화[8,9]	가능	×	○	암호 1회
XOR기반[10,11]	불가능	○	○	비트연산
제안 기법	불가능	○	○	비트연산

○:제공. ×:제공안함.

서로 다른 메시지가 전달된다. 또한 임의로 선택된 두개의 부분ID(PID_{1L}과 PID_{2R}) 가 매번 변화하고 또한 그들의 XOR연산 한 결과도 매번 서로 다르다. 그러므로 정보를 교환에서 불변메시지를 통한 태그의 위치 추적은 불가능하다. 하지만 태그의 SID를 알고 있을 경우 매번 서로 다른 메시지가 전송된다 해도 태그의 위치를 추정할 수 있다. 이것은 특수 목적(법적수사)의 태그추적은 관리자의 권한위임을 통하여 가능함을 제시한다.

4) 사용자 프라이버시 보호: 사용자 프라이버시는 주로 태그의 소유자의 위치정보나 태그정보 누출을 말한다. 위에서 설명한바와 같이 제안 프로토콜에서는 동일한 리더기가 동일한 태그에 대한 인증이라 해도 난수 및 랜덤 한 두 부분 ID의 XOR연산을 통하여 정보은닉 및 매번 서로 다른 인증메시지를 교환으로 태그의 위치 노출과 태그정보유출을 막을 수 있어 사용자 프라이버시가 보장된다.

표 1은 기존 인증기법과 비교분석한 결과이다. 분석결과를 보면 제안 프로토콜은 안전성 기능이 기존기법에 기능에 비하여 확장되었음을 알 수 있다. 즉 제안 프로토콜은 다양한 공격에 안전하며 또한 계산 측면에서도 효율적임을 알 수 있다.

4.2 효율성 평가

RFID 시스템에서는 전력소비, 처리시간, 저장 공간 및 게이트(gate)수 등이 비용계산의 주요변수로 작용한다. 따라서 저비용 RFID 시스템의 구현에 있어서 위의 3가지요소를 줄이는 것이 매우 중요하다. 기존에 제안된 기법에서는 주로 해쉬함수와 암호화 기법을 사용하여 구현하는데 20000~30000gate 비용이 든다. 그 외 최근에 제안한 비트연산을 이용한 Juels기법[10]과 Eunyoung 기법[11]은 500~5000gate의 비용이 들어 해쉬함수나 암호화기법을 보다는 효율적이다. 그러나 이 두 가지 기법 역시 EPC 표준의 Class 1에 속하는 읽기전용 태그에는 적용할 수 없다. 표 2는 기존 Juels기법[10]과 Eunyoung 기법[11] 및 제안프로토콜들의 태그에서의 비용을 비교분석한 결과이다.

표 2. 기존 프로토콜과의 효율성 비교분석

	Juels[10]	Eunyoung[11]	제안기법
태그의 연산량	$3km(XOR)$	$8(XOR)$ +4(덧셈)	3 (XOR)
태그의 데이터양	l*($3km$+$3k$)	$8l$	$1l$
태그의 추가공간	필요	필요	불필요
태그의 쓰기연산	필요	필요	불필요

k:래덤 값 개수, m:비밀 값 수.l:태그의 비트 수.

표 2에서 알 수 있는바 Juels 기법에서는 $3km$ (여기서 k는 각 세션에 사용되는 랜덤 값 개수, m는 태그에 저장된 k개 랜덤 값을 한 조로한 비밀 값 개수.l:태그의 비트 수)번의 XOR연산을 수행하고 Eunyoung 기법에서는 8번의 XOR연산과 4번의 덧셈을 수행하며 제안프로토콜에서는 3번의 XOR만 수행한다. 따라서 Juels 기법과 Eunyoung 기법에 비하여 태그의 연산량이 절반이 줄었으며 또한 쓰기연산과 추가적 저장 공간 필요로 하지 않으므로 저비용 읽기전용 RFID 태그의 활용에 적합하다. 기존 읽기전용으로 태그를 이용한 RFID시스템의 정보보호는 단지 물리적 접근으로만 가능한 것을 제안 프로토콜에서는 소프트웨어적 방법으로 해결하였음은 기존 기법보다 우월하다는 것을 입증할 수 있다.

V. 결 론

RFID기술은 기존 바코드 기술에 비해 인식속도가 빠르고, 저장 공간이 크며 무선인식 등 장점을 갖고 있어 사회의 각 분야에 활용되고 있다. 그러나 기존 RFID시스템은 비용문제, 무선 환경의 보안 취약성 및 프라이버시 침해와 같은 새로운 보안문제점이 발생하고 있다. 특히 읽기전용 태그를 이용하는 RFID시스템에서는 물리적 방법으로만 정보보호 문제를 해결하고 있다.

이 논문에서는 간단한 XOR연산과 부분 ID를 이용하여 다양한 공격에 안전하며 읽기전용태그에도 적용 가능한 저비용 상호인증 프로토콜을 제안하였다. 이 인증프로토콜은 기존 프로토콜에 비하여 자원소비의 최소화 하였고 또한 도청, 위장 및 프라이버시 침해와 같은 문제점을 해결하였음을 기존 기법과의 비교분석을 통하여 입증 하였다.

참 고 문 헌

〔1〕 S. A. Weis, "Radio-frequency identifica tion security and privacy", Master's thesis, M.I.T. 2003

〔2〕 S. A. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", In First International Conference on Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, Springer-Verlag.

〔3〕 A. Juels and R. Pappu, "Squealing Euros : Privacy protection in RFID-enabled banknotes", Financial Cryptography'03, LNCS 2742, pp. 103-121, Springer-Verlag

〔4〕 D. Molnar, A. Soppera, and D. Wagner. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In B. Preneel and S. Tavares, editors, Selected Areas in Cryptography-SAC 2005, Lecture Notes in Computer Science. Springer-Verlag, 2005.

〔5〕 D. Henrici, P. Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. PERCOMW '04, pp.149-153, IEEE, 2004

〔6〕 M. Ohkubo, K. Suzuki, and S. Kinoshita (2003), "A Cryptographic Approach to "Privacy-Friendly" tag", RFID Privacy Workshop

〔7〕 Junko Yoshida, "RFID Backlash Prompts 'Kill' Feature," EETimes. April 28, 2003,

〔8〕 A. Juels, R. L. Rivest and M. Szydlo(2003), "The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy", 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103-111

〔9〕 P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal reencryption for mixnets. In T. Okamoto, editor, The Cryptographers' Track at the RSA Conference-CT-RSA, volume 2964 of Lecture Notes in Computer Science, pages 163-178. Springer-Verlag, 2004.

〔10〕 A. Juels, "Minimalist cryptography for low-cost RFID tags", In 4th Intel. Conf. on Security in Communication Networks-SCN 2004 vol. 3352 LNCS. pp. 149-164.

〔11〕 Choi, Eun Young and Lee, Su Mi and Lee, Dong Hoon, "Efficient RFID Authentication protocol for Ubiquitous Computing Environment" In International Workshop on Security in Ubiquitous Computing Systems - secubiq 2005, Volume 3823 LNCS, pp. 945-95.

이 영 진 (Yong-zhen Li) 준회원

1994년 6월 중국 연변대학교 물리학과 이학사

1997년 6월 중국 연변대학교 물리학과 이학석사

2003년 3월~현재 충북대학교 전자계산학과 박사과정

<관심분야> 정보보호, 네트워크 보안, 유비쿼터스 보안

문 형 진 (Hyung-Jin Mun) 정회원

1996년 2월 충남대학교 수학과 졸업

2002년 2월 충남대학교 수학과 이학석사

2003년 3월~현재 충북대학교 전자계산학과 박사과정

<관심분야> 암호학, 정보보호, 프라이버시 보호

정 윤 수 (Yoon-su Jeong) 정회원

1998년 2월 청주대학교 전자계산학과 이학사

2000년 2월 충북대학교 전자계산학과 이학석사

2003년 3월~현재 충북대학교 전자계산학과 박사과정

<관심분야> 암호 이론, 정보보호, 네트워크 보안, 이동통신 보안

이 상 호 (Sang-ho Lee) 정회원

1976년 2월 숭실대학교 전자계산학과 졸업
1981년 2월 숭실대학교 전자계산학과 공학석사
1989년 2월 숭실대학교 전자계산학과 공학박사
1981년~현재 충북대학교 전기전자컴퓨터공학부 교수

<관심분야> Protocol Engineering, Network Security, Network Management, Network Architecture